Data Storage Location [1]

Topics:
data storage location [2], cloud [3], procurement [4]

SS-15-002.01 Data Storage Location

Issue Date: 12/15/2014

Effective Date: 12/15/2014

PURPOSE

When a data storage facility is not located in the United States (US), there is an increased risk that the data stored offshore will be subject to the sovereign control of the country where the data is located. Offshore data storage can occur in several ways as follows:

- A cloud service provider, such as one who provides Software as a Service (SaaS) applications, stores State data on servers in another country.
- A third-party service provider, a contractor that hosts an application utilized by State employees via network links, uses a data center in another country or uses a US data center but uses storage in another country.
- A Cloud or third-party service provider uses facilities in another country for disaster recovery, capacity management or other purposes.

There are significant risks to offshore data storage as follows:

- The physical location of data is often critical in determining which sovereign nation controls that data. There is no international standard that governs the question of data sovereignty. Rather, disputes about the control of data are resolved on a case-by-case basis, often depending upon geography and/or economic factors.
- Government authorities, courts, administrative bodies where a server is located may have more access or different access to State data than one expects in the United States.
- The potential for the exploitation of an insider threat increases whenever non-American staff has access to American data. Local cybersecurity capabilities of the hosting country and its internet service providers may be weaker than they are here in the United States.

In general, principles of good governance and caution require the State of Georgia to control its own destiny. Third-party hosted applications and cloud based services might utilize servers located anywhere in the world unless restricted by the State?s contract with the service provider.

This standard requires all State data to be stored only on servers within the United States in order to reduce the jurisdictional and security concerns that attend offshore data storage.

STANDARD

When using contracted cloud services, a State agency must include appropriate contract language to retain data ownership and ensure appropriate measures of confidentiality, integrity and availability. This becomes more critical as the data?s security categorization increases.

1. All State data must be processed, stored, transmitted and disposed of onshore (within the jurisdiction of the United States).